UNIVERSIDADE DE BRASÍLIA
CIÊNCIA DA COMPUTAÇÃO
ESCOLA DE EXTENSÃO
Prof. Pedro A. D. Rezende

# REDES PRIVADAS VIRTUAIS COM IPSec

Dêner Lima Fernandes Martins
Brasília – DF – 11-agosto-2000

# SUMÁRIO

# Redes Privadas Virtuais com IPSec

## 1 – Introdução

Com a recente explosão da Internet comercial, Intranets, Extranets, aplicações B2B (*Business to Business*), o uso das redes privadas virtuais (**VPN** –***V****irtual* ***P****rivate* ***N****etwork*) e de protocolos de rede que oferecem mais segurança na comunicação tornaram-se peças estratégicas na implementação dessas idéias. É cada vez maior o número de fabricantes oferecendo sua própria solução para as VPN. Isso tem trazido confusão a um mercado que é por si só bastante heterogêneo.

Um padrão de comunicação segura tem-se sobressaído dentre outros, é o IPSec (***IP Sec****ure*). Mas não sem motivo, pois o IPSec é o protocolo que oferece a estrutura mais completa para VPNs. Os outros protocolos estão cada vez mais se aproximando dele para seus serviços de segurança. O IPSec oferece conexão de rede local para rede local, e de cliente para rede local, o que faz com que os outros protocolos sejam descritos comparando-se suas características com as do IPSec. Esse protocolo está sendo adotado por um número cada vez maior de fabricantes de equipamentos de rede e programas para computador, tornando-se cada vez mais o padrão *de facto*.

Este trabalho apresenta ao leitor uma visão breve da tecnologia das VPN e do protocolo IPSec. Será explicada ainda a sua utilização no mundo real das redes de computadores.

## 2 - Redes Privadas Virtuais

Podemos definir uma VPN como uma emulação de uma rede privativa de longa distância usando redes IP, tais como, a Internet que é uma rede pública, ou backbones IP privados. As VPN podem ser vistas como redes virtuais operando sobre redes reais (IP, ATM, Frame Relay, etc) [4]. Entre os fatores que podemos citar para o uso desta tecnologia é a capilaridade da Internet, redução dos custos de telecomunicações, o esconder de olhos alheios determinada parte do tráfego da rede de uma organização, e a facilidade de instalação. O tráfego da VPN necessita ser opaco, i.e., não pode haver vazamentos de pacotes para fora do “túnel” criado pelo protocolo de rede específico da VPN [2].

### 2.1 – Tipos de VPN

As VPN podem ser baseadas em conexão usuário-gateway e gateway-gateway. Nó podemos dividir as VPN em quatro tipos básicos [4]:

- ***V**irtual **L**eased **L**ine* – **VLL**.
- ***V**irtual **P**rivate **R**outed **N**etwork* – **VPRN**.
- ***V**irtual **P**rivate **D**ial **N**etwork* – **VPDN**.
- ***V**irtual **P**rivate **L**AN **S**egment* – **VPLS**.

### 2.1.1 – Virtual Leased Line Network

O primeiro tipo de VPN é a VLL (e o mais simples), onde dois usuários estão conectados por um "túnel" IP que emula um circuito físico dedicado ou uma linha privada. O backbone IP é usado como entidade de enlace, transporte fim-a-fim, de forma transparente para o backbone. Vários túneis do tipo VLL podem começar e terminar em uma mesma estação.

### 2.1.2 – Virtual Private Routed Network

O segundo tipo é a VPRN corresponde à emulação de uma **WAN** (***W**ide **A**rea **N**etwork*) com vários *sites* usando protocolo IP. Uma WAN se caracteriza pela necessidade de configuração de endereços no nível de usuário da VPN e de provedor de serviço de rede. Ela consiste de uma rede de topologia não organizada (rede *mesh*) entre os roteadores do provedor de serviço. O VPRN trabalha enviando os pacotes na camada 3. Cada protocolo de rede necessita ter uma VPRN, ou eles são encapsulados no protocolo IP. O VPRN permite também controle de tráfego nos nós da rede evitando congestionamento.

### 2.1.3 – Virtual Private Dial Network

O terceiro tipo é a VPDN que permite aos usuários terem acesso remoto via linha discada (***PPP** - **P**oint–to-**P**oint **P**rotocol*). Neste caso a autenticação do usuário é muito importante, a qual pode ser feita por meio de um servidor Radius, por exemplo. Esta forma de VPN permite o tunelamento com os protocolos IPSec ou L2TP. Quando o provedor de acesso discado impõe o uso de VPN como sendo obrigatório, esta forma é também chamada de tunelamento compulsório, i.e., sem o uso da VPN o usuário não consegue acesso aos recursos da rede do provedor. Quando o usuário faz uma VPN com um *site* remoto sem o envolvimento dos nós de rede intermediários, diz-se que o túnel é voluntário.

### 2.1.4 - Virtual Private Lan Segment

O quarto tipo de VPN é a VPLS, e emula um segmento de rede local usando o backbone IP. A VPLS é utilizada para prover o serviço de LAN transparente, e oferece serviço semelhante à emulação de LAN do ATM, onde segmentos de rede fisicamente afastados trocam pacotes pelo backbone ATM como estivessem no mesmo segmento de colisão de rede. A VPLS também oferece completa transparência aos protocolos, com tunelamento multiprotocolar, e suporte a broadcast e multicast [3].

Há vários protocolos de rede que podem ser utilizados para formar uma VPN. Entre eles podemos citar o L2TP, MPLS, IPSec, GRE e IP/IP. Neste trabalho descreveremos o IPSec.

## 3 - IPSec

A versão "4" do protocolo **TCP/IP** (***T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol*), utilizado hoje na Internet, não possui nenhuma característica de segurança inerente. No início da Internet, quando somente universidades e instituições de pesquisa e governamentais dos E.U.A. estavam conectadas entre si, a segurança não era uma questão tão crucial como nos dias de hoje. Com a variedade de aplicações comerciais para a Internet crescendo, o IETF (***I**nternet **E**ngineering **T**ask **F**orce*) criou o grupo IP Security para endereçar o problema de segurança a nível de pacote [5].

### 3.1 – Protocolos de Segurança

Os primeiros protocolos compreendendo IP seguro, autenticação e cifragem de datagramas foram publicados em 1995 nas RFC1825 à RFC1829 (***R**equest **F**or **C**omment* – **RFC**). Esses protocolos estabeleceram os fundamentos da arquitetura do IPSec, foram posteriormente superpostos pelas RFC2401 à RFC2406, entre outras. Estas RFC previam o uso de dois tipos de cabeçalhos para serem utilizados no datagrama IP.

### 3.2 – Datagramas IP

Os pacotes ou datagramas IP são a unidade fundamental na comunicação de redes IP. Foram definidos dois cabeçalhos para o IPSec, o de autenticação (AH) e o de encapsulamento de segurança de carga útil (ESP), que lida com a criptografia do conteúdo do pacote. O IPSec é compatível com o IP versão "6", pois seu desenvolvimento foi feito paralelo ao do IPv6. Como a adoção do IPv6 está sendo muito lenta, o IPSec foi adaptado para o uso na versão 4 do TCP/IP [7]. A figura 1 mostra os cabeçalhos do IPv4 e IPv6, antes de aplicar o IPSec.

| Campos diversos do cabeçahos IP | Endereço IP de origem | Endereço IP de destino | Outros cabeçalhos |
|---|---|---|---|

**IPv4**

| Vários cabeçalhos | Próximo cabeçalho | No. de pulos | Endereço IP de origem | Endereço IP de destino | Próximo cabeçalho | Comprimento de cabeçalho | Dados | Cabeçalhos de alto nível |
|---|---|---|---|---|---|---|---|---|

**IPv6**

Figura 1

## 3.3 – Implementações do IPSec

As aplicações atuais que querem utilizar o IPSec devem incluir pilhas especiais. À medida que mais e mais redes mudarem para IPv6, a necessidade de utilizar pilhas compatíveis com IPSec será cada vez menor. Há várias formas de implementação para o IPSec, desde o servidor, até roteadores ou firewalls. Os tipos mais freqüentes são [7]:

- Integração do IPSec na implementação nativa da pilha TCP/IP. Isto requer acesso ao código fonte, e pode ser implementado tanto em servidores como em gateways de segurança.
- Implementação chamada como ***B****ump-****I****n-****T****he-****S****tack* (**BITS**), onde o IPSec é implementado sob a pilha TCP/IP já existente, entre a camada IP nativa, e o driver de rede local existente. Acesso ao código fonte neste caso não é necessário, fazendo desta implementação o tipo ideal para sistemas legados. Esta implementação é usualmente empregada em servidores.
- Implementação chamada como B*ump-****I****n-****T****he-****W****ire* (**BITW**), quando se faz uso de dispositivo físico dedicado para criptografia (*crypto-processor*) em sistemas militares e comerciais dedicados. Normalmente o dispositivo é endereçável na camada IP, e pode ser encontrado em gateways e servidores. Quando o BITW é implementado em um único servidor, ele é análogo ao BITS. Quando o BITW é implementado em roteador ou firewall, ele deve operar como gateway de segurança.

## 3.4 – Protocolos Criptográficos

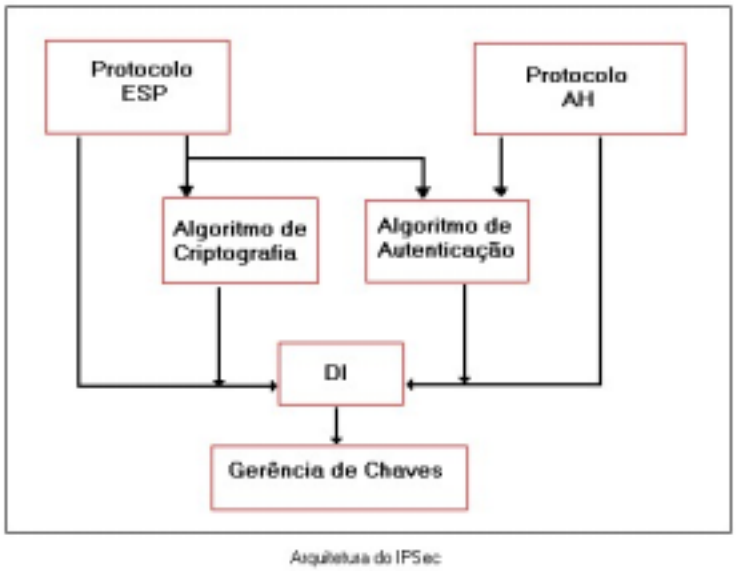
O IPSec foi construído baseado em determinados padrões de criptografia para prover confidencialidade, integridade e autenticação, como exemplo [9]:

- Protocolo Diffie-Hellman para troca de senha secreta entre duas partes quaisquer pela rede pública;
- Criptografia de chave pública para assinar as trocas pelo Diffie-Hellman para garantir as identidades das partes e evitar o ataque conhecido como “homen do meio”;
- DES, 3DES e outros algoritmos para criptografia dos dados;
- Algoritmos de resumo digital (hash) para autenticação dos pacotes, como HMAC, MD5 e SHA-1;
- Certificados digitais para validação de chaves públicas.

## 3.5 - Arquitetura do IPSec

O uso das tecnologias de criptografia foram cuidadosamente traçados nas RFC citadas acima, e em suas posteriores atualizações. A figura 2 mostra as relações entre os componentes da arquitetura do IPSec. Os componentes principais são o cabeçalho de autenticação (**AH**), o protocolo de segurança (**ESP**) e o gerenciamento de chaves. O projeto do AH e do ESP são modulares, o que

possibita o uso de novos algoritmos à medida que forem surgindo no mercado, como o da curva elíptica. Para padronizar os parâmetros de uma determinada transação segura (***S**ecurity **A**ssociation* – **SA**), o IPSec usa o conceito de **D**omínio de **I**nterpretação - **DI**, no qual os algoritmos criptográficos, tamanho de chaves, formato das chaves etc são definidos a priori, quando no estabelecimento da conexão segura.




Arquitetura do IPSec

Figura 2

Cada fase da comunicação segura requer uma SA. Assim, para a autenticação é necessária uma SA, e para a criptografia dos dados outra SA. Mesmo que o mesmo algoritmo utilizado seja o mesmo, os conjuntos de chaves são diferentes. Pode-se pensar na SA como um contrato com quem quer que esteja do outro lado da rede. A desvantagem da SA é que a mesma só pode ser utilizada para transferência de dados em um sentido, i.e., sendo necessário o uso de duas SA para a transferência de dados de forma bidirecional.

O cabeçalho de autenticação normalmente é colocado entre os campos IP e TCP, e nenhuma modificação é feita nos dados do pacote (*payload*). O cabeçalho AH tem cinco campos: próximo cabeçalho, comprimento da parte de dados, índice de parâmetros de segurança -**SPI**, número seqüencial e dados de autenticação.

O SPI especifica para o recipiente do pacote que grupo de protocolos de segurança o remetente está utilizando. Para fazer a atenticação dos dados, o protocolo utilizado é o HMAC (*Hash-based Message Authentication Code*) acoplado com o MD5 (desenvolvido pela RSA), ou com o SHA-1. O MD5 (*Message Digest version 5*), que produz um resumo fixo de 128 bits, está deixando de ser utilizado, pois foram descobertos alguns tipos de ataques de colisão. Atualmente, o algoritmo preferido é o SHA-1 (*Secure Hash Algorithm modified*) desenvolvido pelo U.S. National Institute for Standards and Technology (NIST),

produz um resumo de 160 bits (ou 20 caracteres), e é tido como mais imune a ataques de colisão. Esta forma de ataque consiste em achar duas mensagens que dão origem a um mesmo *hash*. A combinação desses protocolos é conhecida como HMAC-SHA-1. Como o campo do autenticador tem somente 96 bits, o hash é truncado após seu cálculo. O AH possui também mecanismo de “anti-replay” para evitar retransmissões de pacotes, prevenindo ataques do tipo Denial of Service - DoS.

O cabeçalho AH faz somente a autenticação do conteúdo do pacote, e seu conteúdo trafega em claro pela rede. Para assegurar a confidencialidade dos dados faz-se necessário usar o cabeçalho ESP. O ESP é responsável pela cifragem dos dados e é inserido entre o cabeçalho IP e o restante do datagrama. Desta forma, os campos de dados são alterados após serem criptografados. Juntamente com o ESP, segue o SPI para informar ao recipiente do pacote como proceder para a abertura apropriada do conteúdo do mesmo. Um contador no ESP informa quantas vezes o mesmo SPI foi utilizado para o mesmo endereço IP de destino. Esse mecanismo previne um tipo de ataque no qual os pacotes são copiados e enviados fora de ordem, confundindo assim os nós de comunicação.

Todo o restante do pacote, com exceção da parte de autenticação, é cifrado (ou criptografado), antes de ser transmitido pela rede. Os algoritmos de criptografia mais utilizados são o DES, 3DES e protocolos proprietários de fabricantes. O ESP também pode ser utilizado para autenticação, com o campo opcional destinado para esse fim. O somatório de verificação (*checksum*) é computado sobre todo o ESP, com exceção do campo de autenticação, e o seu comprimento varia de acordo com o algoritmo usado. A autenticação do ESP é diferente da fornecida pelo AH, porque ela não protege o cabeçalho IP que precede o ESP, embora proteja um cabeçalho IP encapsulado em modo Túnel. O AH, por sua vez, protege este cabeçalho externo, juntamente com todo o conteúdo do pacote ESP. As duas autenticações não são utilizadas simultaneamente por questão de economia de processamento.

## 3.6 – Modos de Funcionamento do IPSec

O IPSec trabalha em dois modos, modo Transporte e modo Túnel. No modo Transporte, apenas o segmento da camada de transporte é processado, i.e., autenticado e criptografado. No modo Túnel, todo o pacote IP é autenticado ou criptografado. O modo Transporte é aplicável para implementações em servidores e gateways, protegendo camadas superiores de protocolos, além de cabeçalhos IP selecionados. O cabeçalho AH é inserido após o cabeçalho IP e antes do protocolo de camada superior (TCP, UDP, ICMP), ou antes de outros cabeçalhos que o IPSec tenha colocado. Os endereços IP de origem e destino ainda estão abertos para modificação, caso os pacotes sejam interceptados. No modo Túnel, apenas o cabeçalho IP externo (com o último endereço de destino e origem) está visível, informando o destino do gateway (roteador, firewall etc), sendo que todo o conteúdo interno fica cifrado [7].

Além de aplicar AH ou ESP a um pacote IP em modo Transporte ou Túnel, o IPSec ainda requer suporte para certas combinações dos dois modos. A idéia é utilizar o modo Túnel para autenticação ou criptografar o pacote e seus cabeçalhos (IP1 ou internos), e então aplicar AH ou ESP, ou ambos, em modo Transporte para ampliar a proteção para o novo cabeçalho gerado (IP2 ou externo). Deve ser observado que em modo Túnel, o AH e o ESP não são usados ao mesmo tempo, pois o ESP tem seu próprio esquema de autenticação. Isso é recomendado apenas quando o pacote interno requer autenticação e cifragem. A figura 3 mostra os cabeçalhos do IPSec, com as possibilidades de modo Transporte e Túnel.

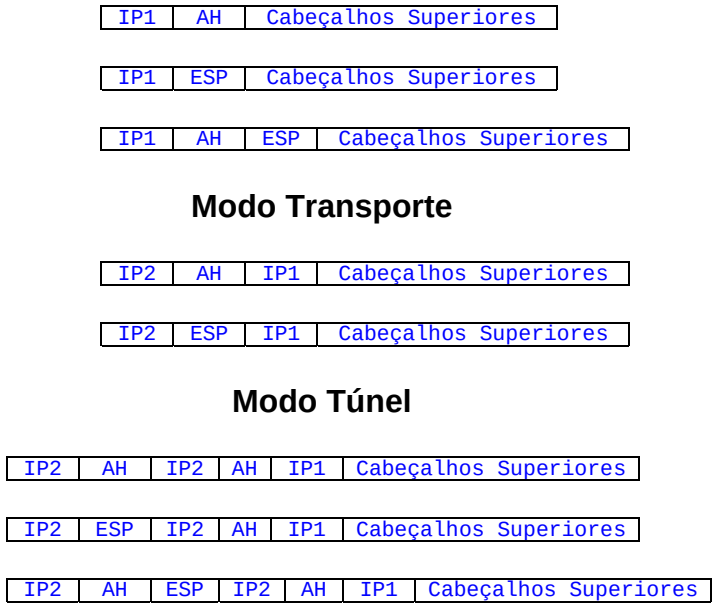


Figura 3

## 3.7 – Gererenciamento de Chaves no IPSec

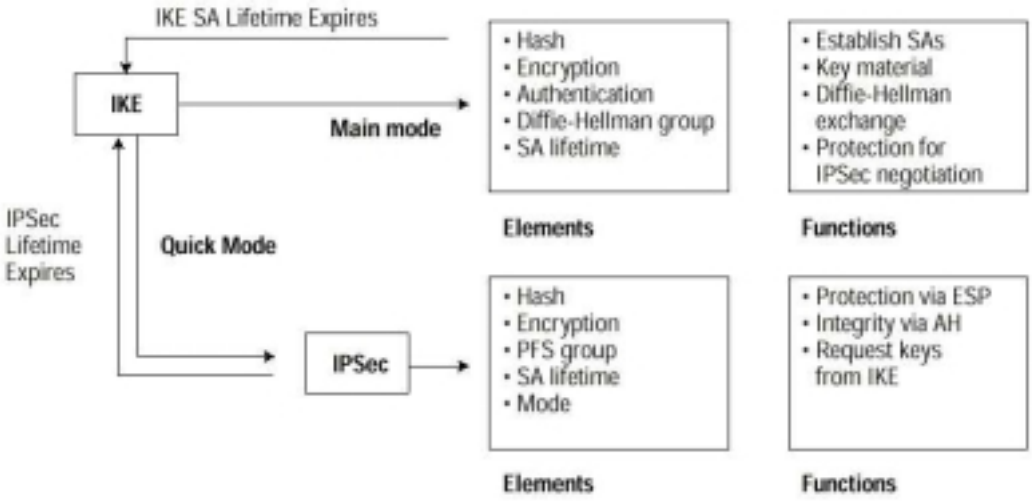
O gerenciamento de chaves pelo IPSec pode ser manual ou automático dependendo do número de sites conectados. O protocolo padrão para gerenciamento automático de chaves utilizado pelo IPSec é o **IKE** (***I**nternet **k**ey **M**anagement*), o qual é a combinação do **ISAKMP** (***I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol*) e o protocolo de Oakley [7]. O primeiro é utilizado como moldura para prover os serviços de autenticação e permuta de chaves. O segundo descreve os vários modos de troca de chaves de criptografia. O IKE opera em duas fases. Na fase um, dois pares estabelecem um canal seguro para realizar as operações do ISAKMP (o ISAKMP SA). Na fase dois, os dois pares negociam os SA de propósito geral.

O protocolo Oakley prove três modos para a troca de informação de chaves e estabelecimento das SA ISAKMP. O modo Principal (*main mode*) faz a fase um de troca do ISAKMP para estabelecimento de um canal seguro. O modo Agressivo (*agressive mode*) é outra forma de realizar a fase um de troca. Este segundo modo é mais simples e rápido que o modo principal, mas em compensação não protege as identidades dos nós envolvidos na negociação, porque ele transmite suas identidades antes do estabelecimento do canal seguro de comunicação. O modo Rápido (*quick mode*) faz a segunda fase de troca negociando um SA para comunicação de uso geral. O IKE possui ainda um outro modo, chamado Novo Grupo (*new group mode*), o qual não se ajusta à fase um ou dois. Ele segue a fase um de negociação, e é utilizado para prover um mecanismo que define grupos privados para troca do tipo Diffie-Hellman.

Para o estabelecimento de uma associação segura IKE, o modo que inicia a negociação deve propor os seguintes itens:

- O algoritmo de criptografia para proteger os dados;
- Um algoritmo de hash para assinatura digital;
- Um método de autenticação para assinar o hash;
- Informação sobre qual grupo a troca Diffie-Hellman deve feita;
- Especificação da função pseudo randômica para fazer o *hash* de certos valores durante a troca de chaves, para verificação. Se nada for especificado, o padrão é a versão HMAC mencionada anteriormente.

A figura 4 mostra esquematicamente os elementos do IKE e IPSec, com as funções de chaves providas por eles.




**Elementos do IKE e IPSec**
Figura 4 [10]

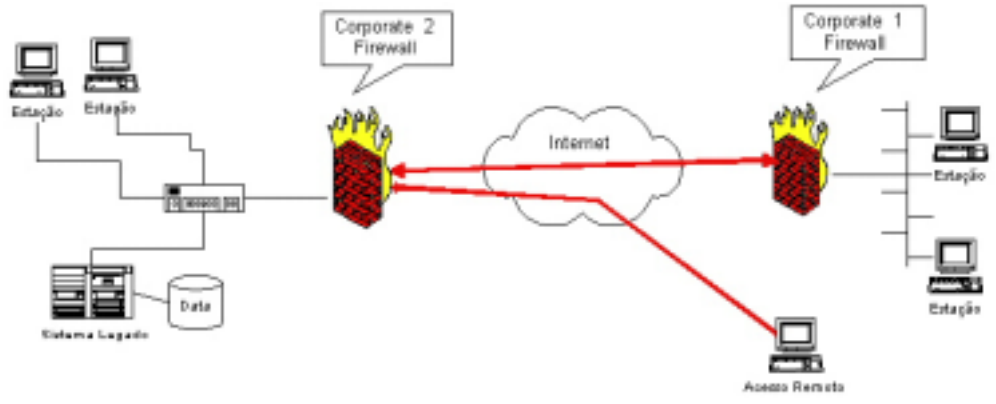
Outro esquema de gerenciamento de chaves existente para o IPSec é SKIP (***S**imple **K**ey **M**anagement for **IP***), utilizado por empresas como Sun Microsystems e Novell. Em vez de utilizar chaves orientadas a sessão, SKIP utiliza chaves orientadas a pacote, as quais são comunicadas em linha com os pacotes. Esse protocolo não faz parte do padrão em uso pelo Grupo de Trabalho do IPSec.

O uso de certificados digitais é outro ponto forte da tecnologia VPN. Muitos fornecedores de certificados digitais fornecem certificados padrão X.509v3 para uso em VPN, sendo sua distribuição feita por intermédio de programas clientes e servidores Web com conectores próprios para esse fim [6]. A autenticação das partes é feita com esse certificado digital. Outro serviço existente para ajudar no gerenciamento das chaves públicas e distribuição das **CRL** (***C**ertificate **R**evocation **L**ist*) é o Serviço de Diretório, com o uso do protocolo **LDAP** (***L**ightweight **D**irectory **A**ccess **P**rotocol*).

## 3.8 Aplicações de VPN com IPSec

O fato do IPSec prover capacidade para garantir a segurança nas comunicações entre redes , torna-o atraente para várias aplicações. As VPN têm sido utilizadas para conectividade entre parceiros de negócio (extranet), acesso remoto seguro, criação de sub-redes virtuais entre matriz e filial, fortalecimento do comércio eletrônico de um modo geral [8].

Na figura 5 vemos um exemplo de uso da VPN. Pode-se estabelecer um túnel entre dois gateways de segurança de duas empresas fazendo uma Extranet; ou ainda entre um cliente remoto e o gateway de segurança para acessar a Intranet corporativa [1].




Exemplo de VPN usando IPSec

Figura 5 [1]

## 4 - Conclusões

A rede privada virtual permite controle de acesso aos recursos de uma empresa pois envolve autenticação, entre outros mecanismos. No entanto, o modo Túnel não impede alguém de bisbilhotar a comunicação entre dois parceiros de negócio e perceber que “algo” está acontecendo quando aumenta o tráfego entre eles [1].

O uso do IPSec aumenta o tamanho do pacote, levando à sua fragmentação e à perda no volume de dados reais trafegados na rede. Há uma proposta de se fazer a compressão do pacote interno antes de ser criptografado, mas isso ainda não se tornou padrão [7]. Apenas alguns fabricantes como o VPNet adotaram esse procedimento.

O IPSec possui como vantagem a sua flexibilidade quanto ao uso, pois ele pode residir em servidores, clientes móveis ou gateways de segurança (firewalls). Caso seja necessário estabelecer a identidade de toda e qualquer conexão, pode-se instalar o IPSec em todos os computadores. As VPN também oferecem a capacidade de **QoS** (***Q****uality* ***o****f* ***S****ervice*), em que a banda disponível para os dados pode ser alocada para determinado tipo de tráfego, de acordo com a prioridade da empresa ou do momento [3].

Deve-se ter cuidado no projeto da rede VPN, principalmente se uma das pontas for um firewall, pois embora esta solução possa oferecer uma boa segurança, o poder de processamento do firewall pode sofre queda de desempenho, devido à divisão de tarefas (VPN x filtro de pacotes).

Com a recente liberação de exportação de programas de criptografia pelo governo dos EUA, o acesso a esta tecnologia ficou mais fácil. O IPSec está se tornando cada vez mais comum entre os fabricantes de computadores e programas. Hoje já é possível fazer uma VPN entre um roteador Cisco e um Firewall-1 da Check Point, ou entre esse último e um notebook fazendo acesso remoto seguro em qualquer lugar do mundo.

O uso do IPSec, cada vez mais difundido no mundo, traz consigo muitas vantagens, entre elas a economia causada pela diminuição do número de linhas alugadas para acesso à Internet, e de comunicação direta entre empresas e suas filiais. A privacidade das comunicações é um fator igualmente decisivo na adoção desta tecnologia, pois ela traz consigo o que há de mais testado na área de criptografia. Espera-se que, nos próximos anos, haja um incremento considerável do uso do IPSec na implementação das VPN.

## 5 - Referências


1. Check Point Software Technologies Ltd., “Redefining the Virtual Private Network”, 1999.
2. Fergusson P., Huston G., “What is a VPN? - Part I”, The Internet Protocol Journal – Cisco, vol. 1, no. 1, 1998.
3. Fergusson, Paul e outros. What is a VPN? - Part II. The Internet Protocol Journal, Cisco, vol. 1, no. 2, 1998.
4. Gleeson, B., “A Framework for IP Based Virtual Private Networks”, IETF RFC2764, 2000.
5. Horak R., “Communications Systems & Networks”, M&T Books, 1999.
6. Kaufman C., Perlman R., Speciner M., “Network Security – PRIVATE Communication in a PUBLIC World”, Prentice Hall, 1995.
7. Kent S., “Security Architecture for the Internet Protocol”, IETF RFC2401, 1995.
8. Stallings W., “IP Security”, The Internet Protocol Journal – Cisco, vol. 3, no. 1, 2000.
9. Stephen K., Atkinson R., “Security Architecture for the Internet Protocol”, IETF RFC1825, 1995.
10. Wilma I., “Deploying IPSec Reference Guide”, Cisco Systems, 1999.


Brasília, 11 de agosto de 2000.


_____
Dêner Lima Fernandes Martins
Curso de Extensão em Criptografia e Segurança na Informática
Departamento de Ciência da Computação – UnB